(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 780 800**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 08717**

(51) Int Cl[7] : **G 07 F 19/00**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 03.07.98.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 07.01.00 Bulletin 00/01.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SAGEM SA Société anonyme* — FR.

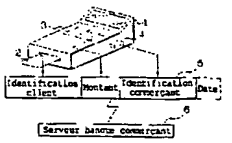
(72) **Inventeur(s) :** SARRADIN JEAN LOUIS.

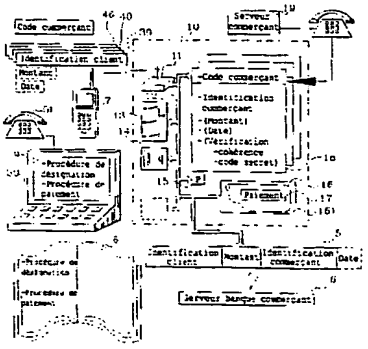
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET CHRISTIAN SCHMIT ET ASSOCIES.

(54) PROCEDE DE PAIEMENT ELECTRONIQUE.

(57) Pour faciliter les paiements électroniques, on transforme un téléphone portable (7) en terminal porteur de paiement. Plus exactement le terminal porteur de paiement est constitué par des circuits des téléphones portables et par des circuits d'un système central (10) d'un opérateur de télécommunications. Cette combinaison de circuits permet de composer d'une manière sûre un message (5) de paiement adressé à un serveur (6) d'un organisme financier.





FR 2 780 800 - A1

Procédé de paiement électronique

La présente invention a pour objet un procédé de paiement électronique. Le but de l'invention est de permettre une très grande diffusion d'un tel mode de paiement, dont l'intérêt est la simplicité et, avec certaines précautions, une grande fiabilité.

On connaît les paiements par carte bancaire, notamment ceux dans lesquelles on prend une empreinte d'un embossage d'une carte de paiement, ou d'une carte de crédit, sur une fiche de paiement et dans lequel l'authenticité du paiement est acquise par la signature du titulaire de la carte au bas de la fiche. Selon les différentes législations, le paiement peut être considéré comme effectué dès l'apposition de la signature ou, dans certains pays, seulement lorsque le titulaire de la carte reçoit à son domicile un relevé des paiements et les accepte, ou tout au moins ne manifeste pas son désaccord d'acceptation. L'embossage révèle des caractères représentatifs de l'identité du titulaire de la carte, surtout de son numéro de compte auprès d'un organisme financier.

Ce type de paiement a été perfectionné par l'apposition à l'arrière des cartes de paiement ou carte de crédit d'une piste magnétique reproduisant, sous une forme mémorisée magnétiquement, les caractères embossés. Un lecteur de piste magnétique d'un terminal de paiement est capable de lire ces caractères et d'éditer la fiche de paiement qui suit par ailleurs un même cheminement d'acceptation.

En cas d'acceptation, un organisme financier du créancier opère les transferts de monnaie scripturale correspondants entre le compte du débiteur auprès d'un organisme financier et un compte du créancier.

Ce type de paiement a été à l'origine d'une fraude assez importante et a dû être sécurisé. Le système de sécurisation retenu a consisté à adjoindre aux informations relatives à l'identité bancaire proprement dite du porteur de la carte (notamment son numéro de compte dans l'organisme financier concerné et éventuellement son adresse), une chaîne de caractères complémentaire constituant une cohérence des informations d'identité proprement dites. Cette cohérence est calculée, en fonction d'un algorithme propre à l'organisme financier, sur la base des informations relatives à l'identité proprement dite. Cette cohérence est constituée par l'adjonction de

cette chaîne de caractères dans la piste magnétique, mais pas dans les caractères embossés. A ce titre cette chaîne de caractères reste inconnue d'un fraudeur de base.

Actuellement les deux systèmes existent, le principe étant qu'un acheteur avisé ne doit effectuer des paiements avec une machine à prendre les empreintes embossées, un sabot, que s'il a une grande confiance dans le vendeur, créancier du paiement, ou ne doit accepter que des paiements magnétiques dans l'autre cas. En effet, pour la prise d'empreintes embossées, il faut surveiller que les fiches de paiement ne soient pas dupliquées par le commerçant, ou un fraudeur. Par exemple, avec une facturette papier dupliquée, un commerçant fraudeur pourrait fabriquer des fausses factures avec un autre sabot, celui d'un autre commerçant complice.

Le lecteur de piste magnétique du terminal de paiement électronique étant relié en temps réel, ou périodiquement en temps différé, à un serveur de données de sa banque, ce lecteur est aisément repérable comme serait par ailleurs repérable par ses facturettes un commerçant fraudeur. Les références de ce lecteur qui sont transmises en même temps que chaque transaction à la banque du créancier désignent le créancier à coup sûr. Mais surtout, l'insertion de la carte dans le lecteur s'effectuant à vue du porteur, celui-ci peut constater qu'elle n'est pas introduite dans un deuxième lecteur. En conséquence ce type de transaction a été rendu plus sûr, du moins du point de vue de la moralité des commerçants. En ce qui concerne les clients, le lecteur vérifie l'authenticité de la carte (contrôle d'authentification). Ensuite la carte contrôle le code confidentiel du porteur via le terminal lecteur. Pour l'authentification, le lecteur peut mettre en œuvre une vérification de la carte avec les informations de cohérence. Le lecteur peut donc détecter les clients fraudeurs.

En ce qui concerne les clients, le système notamment par carte à puce permettant d'authentifier le porteur de la carte par composition d'un code secret permet, bien mieux qu'une signature qui peut être imitée, de vérifier que la carte n'a pas été volée. Pour simplifier, on retiendra que le terminal de paiement, au moment où une carte à puce lui est introduite, après l'authentification, lance une procédure de code secret. Les échecs de cette procédure sont comptés. Au-delà d'un nombre limité d'échecs (trois en général) la carte à puce est invalidée. En cas d'adéquation, la transaction

peut être menée à terme.

Dans tous les cas évoqués ci-dessus le paiement nécessite la présence du commerçant (ou au moins du terminal de paiement de ce commerçant), de la carte de paiement du débiteur et de la présence du débiteur lui-même. Or cette concomitance n'est pas acquise dans le domaine de la vente par correspondance que celle-ci soit réalisée par téléphone, notamment par minitel en France, ou même par Internet. En effet dans ce cas il n'y a pas de terminal de lecture magnétique, ou électronique, pour lire des informations d'identité du débiteur ainsi que des informations de cohérences, qui accompagnent le cas échéant ces informations d'identités.

En pratique, pour de telles transactions il est demandé au débiteur de composer sur un clavier (celui d'un combiné téléphonique, d'un micro-ordinateur relié sur Internet, ou d'un minitel) les 13, 16 ou 19 ou autres caractères numériques embossés de son compte en banque (qui sont par ailleurs représentatifs également de la banque dans laquelle il a un compte), ainsi que d'une manière complémentaire ceux d'une date de validité. On retombe alors avec ce mode de paiement dans les difficultés des fraudes évoquées ci-dessus. En effet quiconque disposant du numéro de carte de paiement d'un tiers peut effectuer des paiements avec ce numéro (et au besoin avec la date de validité), en se faisant livrer à un endroit quelconque des biens ou des services achetés.

Par ailleurs les informations de cohérence ne sont pas disponibles pour les usagers, ils les ignorent, et même leur propre banque refusera de les leur donner. En conséquence, sans terminal de paiement autorisé par l'organisme financier, c'est-à-dire relié à cet organisme financier périodiquement ou en temps réel, il n'est pas possible d'effectuer des paiements sûrs, sans risque pour le débiteur de voir sa carte utilisée par des fraudeurs.

Dans le domaine de la vente par correspondance, notamment en France avec l'usage du minitel, l'information de cohérence inconnue des usagers peut être remplacée par une relation contractuelle préalable. Ainsi, une personne identifiée par son adresse et éventuellement son numéro de compte en banque dans le fichier de l'organisme de vente par correspondance est également doté d'un numéro de contrat attribué par l'organisme de vente par correspondance. Ce numéro de contrat n'est pas le

code secret de la carte bancaire et n'est pas non plus la chaîne de caractères de cohérence ignorée. Mais il constitue un substitut de cette information de cohérence puisque, sans ce numéro de contrat la carte de paiement ne pourra pas être utilisée. En donnant son numéro de contrat, le voleur se désigne et c'est un bon moyen pour éviter sa fraude avec des cartes de paiement volées.

Il reste donc le problème de toutes les ventes par correspondance, vente sur catalogue, ou vente par Internet, dans lesquelles l'acheteur n'a pas préalablement pris contact avec l'organisme de vente par correspondance pour se faire attribuer un numéro de contrat. Les seules solutions qui sont offertes dans ce cas consistent pour l'acheteur à diffuser les références de sa carte de paiement, avec les risques de spoliation envisagés ci-dessus.

Selon l'invention ce problème va être résolu simplement en utilisant pour le paiement un téléphone mobile et, dans une solution principale, les circuits de gestion des communications d'un opérateur central de télécommunications auxquels l'utilisateur est affilié par abonnement pour constituer un message de transaction à établir : pour jouer le rôle du terminal de paiement. Ainsi, par exemple au moment de la souscription de son abonnement, cet utilisateur demandera à incorporer dans les circuits de son téléphone mobile, ou d'une carte à puce ou d'un jeton à puce utilisé avec ce téléphone mobile, des informations relatives à son identité (son numéro de compte en banque essentiellement) et de préférence également les informations de cohérence de sa carte bancaire. En quelque sorte le téléphone mobile comportera de ce point de vue une duplication de sa carte de paiement. Si l'utilisateur perd son téléphone mobile, ce téléphone mobile est néanmoins protégé par son propre code secret de démarrage comme le serait une carte à puce.

Au moment d'une transaction, l'utilisateur composera un numéro de téléphone spécifique de paiement, qui n'aboutit, dans cette solution principale, chez aucun interlocuteur si ce n'est à une fonction particulière dans les services centraux de l'opérateur. A cet instant la communication établie permet d'exécuter automatiquement un programme spécifique. Au cours de ce programme spécifique, l'utilisateur compose et fait envoyer un code relatif à l'identité du commerçant auprès duquel il veut faire une acquisition. Eventuellement ce code est relatif à la transaction elle-même si

celle-ci est identifiée par ailleurs. Les services centraux de l'opérateur de télécommunications composent alors un message de paiement. Ce message de paiement est établi sur la base de l'identification du client débiteur (connue par le téléphone mobile et communiquée automatiquement à l'opérateur de télécommunications) et sur la base d'un code de créancier (communiqué par l'utilisateur au moment où il envoie le code de commerçant après composition). Les services centraux de l'opérateur retrouvent à partir de ce code de créancier, ou de ce code de transaction envoyé par l'utilisateur du téléphone, l'identité du commerçant et éventuellement un montant de transaction. Ce montant peut être autrement composé par l'utilisateur du téléphone, à moins qu'il ne corresponde à la transaction.

Une fois que ce message de paiement est composé, les services centraux de l'opérateur de télécommunications effectuent en plus l'envoi du message correspondant à un organisme financier qui correspond soit au débiteur, soit au créancier, mais de préférence au créancier. Cet organisme financier effectue alors la transaction comme dans le cas des paiements avec des terminaux électroniques communs. En quelque sorte, en agissant ainsi l'opérateur de télécommunications se substitue, avec tous ses services, à un terminal de paiement électronique. Ce terminal de paiement électronique ainsi réalisé est particulier en ce sens qu'il est universel. Il concerne tous les commerçants et tous les organismes financiers. Il suffit seulement que l'opérateur puisse être en relation avec les différents organismes financiers. Deux autres variantes seront également décrites par la suite dans lesquelles la constitution du message de paiement va être partagée.

L'invention a donc pour objet un procédé de paiement électronique dans lequel

- on complète un message de paiement comportant une information d'un montant d'une transaction, une information d'identité d'un débiteur de ce montant et une information d'identité d'un créancier de ce montant,

- on envoie ce message à un serveur de données d'un organisme financier,

- le serveur de cet organisme financier opère des transferts de monnaie scripturale correspondant à ce paiement,

caractérisé en ce que

- on émet à partir d'un téléphone mobile, et en direction d'un système central d'un opérateur, l'information d'identité du débiteur,

- on constitue, dans ce système central, le message de paiement à partir de l'information d'identité de débiteur reçue, et d'une information d 'identité de créancier,

- on envoie le message ainsi constitué à un serveur de données d'un organisme financier.

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont données qu'à titre indicatif et nullement limitatif de l'invention. Les figures montrent :

- Figure 1 : la représentation schématique d'un procédé de paiement électronique de l'état de la technique ;
- Figure 2 : une représentation schématique des moyens mis en œuvre dans le procédé de l'invention ;
- Figure 3 : une représentation schématique des moyens du téléphone mobile mis en œuvre dans le procédé de l'invention ;
- Figure 4 : un organigramme de déroulement des étapes du procédé de l'invention ;
- Figure 5 : une présentation comparative des différentes variantes de l'invention.

La figure 1 montre les moyens utilisés dans l'état de la technique pour effectuer un paiement électronique. Dans un terminal 1 de paiement électronique, on insère une carte 2 de paiement, carte à puce ou carte magnétique. Avec un clavier 3 du terminal 1, le commerçant compose le montant de la transaction. En pratique cette opération comporte une authentification de la carte et une authentification du porteur par une composition de code secret mais qui n'est pas pertinente au premier chef ici. Ce faisant un message 5 de paiement ainsi constitué par le terminal 1 comporte l'identification du débiteur, (c'est-à-dire le client), le montant de la transaction, et l'identification du créancier (c'est-à-dire le commerçant). L'identification du débiteur est prélevée dans la carte 2. L'identification du créancier est prélevée dans le terminal 1. Le montant est composé au clavier. D'autres informations sont également données, notamment la date de la transaction, la date de validité de la carte de paiement 2, ainsi que d'autres types d'informations. Dans l'identification client, figure l'identification

proprement dite et, de préférence, la chaîne de caractères de cohérence qui authentifie intrinsèquement l'identité du client. Dans l'identification du commerçant on retrouve les mêmes éléments. Ceux-ci sont disponibles dans une mémoire 4 du terminal 1.

Le terminal 1 est relié par une ligne téléphonique (filaire, hertzienne ou autres) avec un serveur 6 de la banque du créancier. Le serveur 6 de cette banque est capable de recevoir le message 5 envoyé, et de traiter la transaction financière qui lui correspond. D'une manière connue, le serveur 6 de la banque du commerçant émet un ordre de prélèvement du compte du client pour le débiter et pour créditer le compte du commerçant qu'elle gère.

La figure 2 montre la modification de cette transaction selon l'invention, notamment pour la rendre accessible avec sécurité à la vente par correspondance. Ce mode de paiement peut toutefois se substituer aux paiements avec terminal 1, si le commerçant l'accepte et s'il s'est organisé en conséquence. On verra par la suite comment, plutôt qu'une substitution pure et simple qui appelle la méfiance du commerçant, celui-ci peut participer avec ses équipements à l'opération de paiement. Dans ces cas, selon l'invention, un client disposant d'un téléphone mobile 7 consulte un catalogue 8 de vente par correspondance ou même consulte une session 9 de connexion sur Internet. Eventuellement il consulte la vitrine d'un commerçant. Il détecte dans ces consultations un bien ou un service qu'il veut acquérir. Les informations qui sont mises à sa disposition par le vendeur sont alors, selon l'invention, essentiellement des indications relatives à une procédure de désignation du bien ou du service acheté, et d'une procédure de paiement.

Ces deux notions ne sont toutefois pas nécessairement complètement séparées, il est possible en effet notamment au cours d'une session Internet 9, qu'un seul produit soit achetable auprès du commerçant, auquel cas la désignation du bien ou du service sera implicitement comprise dans la désignation du commerçant. On verra par la suite comment peut être menée à terme, avec toutes les variantes possibles, la procédure de désignation du bien ou du service choisi par le client. Pour l'instant, pour ce qui concerne l'invention seul est important le fait que soit mis à la disposition de l'acheteur une procédure de paiement.

Cette procédure de paiement peut comporter une succession

d'opérations à effectuer par l'acheteur mais elle comportera essentiellement, selon l'invention, l'envoi d'un code commerçant. En effet, comme on l'a dit ci-dessus le terminal de paiement auquel on va s'adresser est un terminal universel, il n'est pas comme le terminal 1 automatiquement muni d'une mémoire 4 avec l'identification d'un commerçant spécifique ni non plus automatiquement connecté à un serveur 6 de données de la banque du commerçant. Par conséquent, dans le catalogue 8 dans la session 9 ou dans sa procédure de paiement, le commerçant doit indiquer un code qui le concerne dans les services de l'opérateur de télécommunications. Ce code pourrait même être l'identification complète du commerçant comme vu plus haut. Il pourra de préférence être plus simple, notamment comporter par exemple un nom commercial suivi, éventuellement, d'un numéro d'article vu dans le catalogue. Ainsi pour une société nommée VPC de vente par correspondance, et pour un article de numéro 0001, le code commerçant pourra être VPC, ou VPC 0001 selon le cas.

Selon l'invention, le téléphone mobile 7 va envoyer, pour le paiement, dans un système central 10 d'un opérateur de télécommunications publiques avec des mobiles, un message comportant essentiellement le code commerçant vu ci-dessus (VPC, ou VPC 0001) ainsi que l'identification client (c'est-à-dire l'identité du client et de préférence la chaîne de caractères de cohérence). D'une manière optionnelle le client enverra avec son téléphone mobile 7 le montant de la transaction et la date de la transaction. Le montant de la transaction et la date de la transaction ne sont pas nécessaires si l'article acheté est déjà identifié implicitement dans le code commerçant. De même ils ne sont pas nécessaires si le commerçant ne vend qu'un seul article. La date peut par ailleurs être apportée dans le message de paiement par l'opérateur.

Pour l'envoi des deux composantes essentielles, le code commerçant et l'identification client, il n'est demandé à l'utilisateur du téléphone mobile que de composer le code commerçant. L'identification client étant préalablement contenue dans les mémoires de ce téléphone mobile sera adjointe au message d'une manière automatique. Après cette composition du code commerçant, le client se met en relation avec le système central 10. A cette fin il dispose d'un numéro de téléphone spécifique.

Le système central 10 de l'opérateur de télécommunications comporte

au moins une station de base 11 en relation avec le téléphone mobile par voie hertzienne, et avec les différents circuits de ce système central par l'intermédiaire d'un bus 12. D'un manière connue ces circuits comporteront des circuits 13 de commutation et des circuits annexes. Les circuits 13 servent à la fonction principale d'un opérateur de télécommunications : à établir des liaisons entre différents interlocuteurs. Les circuits annexes peuvent être variés et comporter par exemple des boîtes vocales 14. Le système central 10 est administré par un processeur 15 qui met en œuvre un programme 16 général. Le programme 16 est contenu dans une mémoire 161 reliée au bus 12. Selon l'invention ce programme 16 sera complété par un sous programme 17 de paiement électronique selon l'invention. Le sous programme 17 a pour objet de reconstituer le message 5 et de l'envoyer à un serveur 6 de données de la banque du commerçant. Le sous programme 17 est la fonction spécifique de paiement lancée chaque fois qu'un accès est effectué sur le numéro de téléphone spécifique.

Dans ce but, le système central 10 comportera une mémoire de paiement 18 dont chaque enregistrement peut être adressé par un code commerçant reçu du téléphone mobile 7. Dans un enregistrement correspondant à un code commerçant, on trouve ainsi une information relative à l'identification du commerçant, notamment à son compte en banque, et à une identification de la banque du commerçant. Cette dernière information sera notamment utile pour, une fois que le message 5 aura été constitué, l'envoyer au serveur 6 de la banque du commerçant.

En variante, la mémoire 18 sera réduite, et ne comportera qu'une identification de commerçant permettant au service central 10 de se connecter, en temps réel ou en temps différé, sur un serveur de données 19 du commerçant afin d'y puiser les informations correspondant à la transaction souhaitée par le porteur du téléphone mobile 7. Ainsi, dans le cas où le code commerçant comporterait les informations VPC 0001, le système central 10 composera un numéro de téléphone (correspondant au commerçant VPC et qu'il connaît dans sa mémoire 18). Ce numéro de téléphone est celui du serveur 19 du commerçant. Par une requête automatique, le système central 10 pourra obtenir de ce serveur 19 d'une part l'identification bancaire de ce commerçant et d'autre part éventuellement le montant de la transaction relative à l'article correspondant 0001.

En variante le processeur 15, en exécution du programme 17, peut apporter la date du jour au message 5 ainsi qu'effectuer la vérification des identifications du client et du commerçant. En effet dans les deux cas il recevra des entités 7 et 19 des identités proprement dites ainsi que les chaînes de caractères de cohérence. Dans une variante préférée également le sous programme 17 pourra lancer une vérification de code secret, pour authentifier le porteur du téléphone mobile. Ou le sous programme 17 pourra faire faire cette vérification par un circuit contenu dans le téléphone mobile 7.

En résumé l'identification client est envoyée par le téléphone mobile 7 au moment de la transaction. L'identification du commerçant est envoyée par le serveur commerçant 19. Elle est envoyée préalablement pour être stockée dans une mémoire 18, ou à la demande, en temps réel ou en temps différé par rapport à l'instant de la transaction. Le montant peut être composé par l'utilisateur du téléphone mobile 7. Il peut être préalablement stocké dans la mémoire 18. Ou encore il peut être envoyé à la demande par le serveur 19. L'avantage d'utiliser le serveur 19, et donc la communication entre le système central 10 et ce serveur 19, pour parfaire la transaction est que le commerçant peut changer de banque comme il veut et que d'autre part le système central 10 n'est pas responsable juridiquement de la transaction puisqu'il ne fait que transcrire des informations qu'on lui donne pour composer le message 5. Dans un enregistrement de la mémoire 18 correspondant à un code commerçant, on trouvera donc de préférence des moyens d'identification du commerçant, avec la chaîne de caractères de cohérence, et des moyens d'identification de sa banque, c'est-à-dire l'expression du protocole de connexion utilisable pour transmettre ensuite le message 5 à cette banque.

La figure 3 montre une modification fonctionnelle d'un téléphone mobile pour le faire fonctionner selon l'invention. Le téléphone mobile 7 comporte d'une manière connue un microprocesseur 20 relié par un bus 21, à une mémoire programme 22, à une mémoire de données 23, à une mémoire de travail 24, à un circuit d'émission réception 25, à un clavier 26, et à un écran 27. Pour la relation avec le monde extérieur, le bus 21 est encore relié à un connecteur 28, de carte à puce ou similaire ainsi qu'à un connecteur d'embase 29. Le connecteur 29 sert la plupart du temps pour recharger une batterie (non représentée) du téléphone mobile. Mais il peut

également servir pour connecter le téléphone 7 à un micro-ordinateur 30. Le micro-ordinateur 30 est par exemple celui à partir duquel on a lancé une session Internet 9. Cependant il ne faut pas confondre la session Internet (qui pourrait, elle aussi, utiliser le téléphone mobile comme moyen de communication), et la session de paiement dans laquelle on met en œuvre le procédé de paiement selon l'invention.

Le connecteur de carte à puce 28 est optionnel quoique correspondant à une solution préférée. En effet celui-ci permet de connecter un circuit à puce 31 amovible comportant lui aussi un bus 32 relié au connecteur 28, un microprocesseur 33, une mémoire programme 34 et une mémoire de données 35.

Dans la mémoire de données 23 figurent diverses informations mais notamment un numéro dit IMSI, pour International Mobile Set Identification, qui permet d'identifier au cours d'une communication du téléphone mobile 7 avec une station de base 11 quel est le poste téléphonique mobile qui est en cours d'utilisation. Par opposition, dans la mémoire 35 figurera un numéro dit SIM correspondant, mais pour l'opérateur de télécommunications cette fois, à l'identité de l'utilisateur du téléphone mobile. Cette identité est en fait ici en correspondance biunivoque du numéro de téléphone affecté par cet opérateur à l'utilisateur de la carte 31. Le circuit à puce 31 est d'ailleurs appelé couramment carte SIM pour cette raison.

Cette mémoire 35 comporte d'une manière connue différentes zones non volatiles dont notamment une zone 36 comportant un code secret. Lors de l'utilisation du téléphone mobile avec la carte 31, au moment de la mise en service, le programme de la mémoire programme 34 vérifie que le code secret composé par l'opérateur sur le clavier 26 correspond bien à celui enregistré dans la zone 36. Il est également connu d'y disposer dans des zones mémoires telles que 37 des numéros de téléphones préférés. L'opérateur peut les faire apparaître sur l'écran 27 et les sélectionner pour une composition automatique sans avoir à frapper tous les chiffres de ces numéros de téléphone. Le numéro de téléphone spécifique pourra en faire partie.

Selon l'invention, et d'une manière préférée, la carte SIM 31 comportera dans la mémoire 35 une zone 38 dans laquelle seront enregistrées les informations relatives aux paiements effectués par le porteur

du téléphone 7. Par exemple dans un enregistrement 39 de la zone 38, on a mémorisé le numéro de la carte VISA du titulaire de la carte SIM 31 dans une première zone 40, et la chaîne de caractères de cohérence correspondant à ce numéro 40 dans une zone 41. Si le titulaire de la carte SIM 31 possède par ailleurs une carte American Express cette indication sera portée dans un enregistrement 42 dans les zones 43 et 44 respectivement. Et ainsi de suite il pourrait y avoir autant d'enregistrements que le titulaire de la carte SIM 31, ou du téléphone mobile, dispose de comptes financiers différents. De même dans un enregistrement 45, on a fait figurer les références d'une société de vente par correspondance VPC 1 et du numéro de contrat souscrit avec elle en zones 46 et 47 respectivement.

Le choix de la carte SIM 31 pour contenir toutes les informations 39 à 47 est préféré parce que ce choix permet à l'utilisateur, détenteur de la carte SIM 31, d'utiliser n'importe quel téléphone mobile 7 pour effectuer la transaction. En outre, il est plus facile pour un opérateur de recevoir ou de modifier des cartes SIM qu'il édite que de modifier des téléphones mobiles. Néanmoins il serait possible d'incorporer, notamment dans les pays où les caractères amovibles des informations de la carte SIM 31 ne sont pas utilisés, ces informations dans la mémoire 23.

Plutôt que d'avoir le prélèvement de l'identification du commerçant dans le centre serveur 19 par l'intermédiaire du système central 10, il est possible, en connectant simultanément le micro-ordinateur 30 sur une session Internet et sur le connecteur 29, ou en gardant en mémoire les résultats de la session Internet, de transmettre sur le bus 21 les informations d'identification du commerçant, et même de montant, à partir du téléphone mobile 7 pour composer le message électronique de paiement 5. Cependant, même dans ce cas le système central 10 est préféré puisque c'est celui-ci qui effectuera en définitive la vérification de cohérence. En outre, les messages 5 sont de toute manière édités par le système 10 pour être transmis au serveur 6 de la banque du commerçant. Surtout la liaison entre le poste téléphonique mobile 7 et le système central 10 n'est pas une liaison Internet en réseau, ouverte à tous, elle est une liaison privée donc nettement mieux protégée. Quand l'opérateur est ainsi impliqué dans le traitement : on définit un protocole d'échange entre le téléphone mobile 7 et l'opérateur. Ce protocole tient compte des différentes options offertes : connaissance

préalable de l'identification du commerçant, prélèvement en temps réel, ou communication par le client.

La figure 4 montre les opérations 48 mises en œuvre pour effectuer la procédure de désignation et les opérations 49 effectuées selon l'invention pour la procédure de paiement. La procédure 48 de désignation n'est pas nécessairement effectuée par la liaison par téléphone mobile, en utilisant le système central 10 montré sur la figure 2. Elle sera de préférence lancée par le micro-ordinateur 30 au cours d'une session Internet 9. La procédure 48 comporte ainsi une étape 50 d'accès aux services du commerçant. Dans ce but l'utilisateur compose par exemple avec un modem 51 (figure 2) de son micro-ordinateur 30 le numéro de téléphone et le code d'accès qui lui permettent de visualiser sur l'écran de son micro-ordinateur 30 les informations utiles à la transaction.

Lorsque l'accès 50 aux services est effectué, une opération d'accueil 52 s'exécute. Dans le cas où il s'agirait d'une session Internet, l'écran du micro-ordinateur 30 va montrer tous les détails de la transaction. Cette visualisation peut être autrement provoquée sur l'écran du téléphone mobile 7. Dans ce cas néanmoins, les informations seront plus laconiques. Eventuellement si on utilise seulement un téléphone, et même pas un téléphone mobile, il peut y avoir un bip sonore montrant que la connexion est établie, ou voire même rien du tout. Dans ce cas la procédure de désignation apparaissant sur le catalogue 8 indique ce à quoi doit s'attendre l'utilisateur client. Après cet accueil le client désigne dans une opération 53 l'article ou le service qu'il veut acquérir. Il suit les indications qui lui sont données à cet effet soit au cours de la session, soit dans le catalogue 8. Cette désignation 53 est suivie d'une prise en compte de commande 54 par le commerçant, éventuellement sous réserve de paiement. L'opération 54 termine la procédure 48 de désignation. Cette désignation 53 et cette prise en compte de commande 54 utilisent des mêmes moyens de visualisation, ou de communication, que l'étape 52.

La procédure de paiement 49 comporte une communication ou un affichage du prix. Comme vu précédemment, celui-ci peut avoir été visualisé sur un écran, communiqué par une boîte vocale, indiqué dans le catalogue 8 ou autre. Cette communication du prix 55 est préalable. La procédure 56 de paiement proprement dite selon l'invention correspond à un sous programme

57 contenu dans la mémoire programme 22 du téléphone mobile 7, ou bien de préférence contenue dans la mémoire programme 34 de la carte SIM 31. Compte tenu du caractère universel du programme 57, celui-ci pourra néanmoins être incorporé dans tous les téléphones mobiles 7. Le programme 57 comportera de préférence une première étape 58 par laquelle le porteur pourra sélectionner celui des enregistrements 39, 42 ou 45 qu'il choisit (compte tenu de ses disponibilités financières sur ses différents comptes) pour effectuer la transaction.

Une fois cette sélection faite, ou au préalable, le programme 57 demandera en une étape 59 au client de taper le code commerçant évoqué ci-dessus. Ce code commerçant est lisible sur le catalogue 8 ou dans la session 9. Une fois les opérations 58 et 59 réalisées, l'utilisateur provoque avec le téléphone mobile 7 l'envoi au numéro de téléphone spécifique, au cours d'une opération 60, de ces différentes informations : identification de client comportant de préférence la chaîne de caractères de cohérence et code commerçant. Cet envoi est provoqué par l'appui sur une touche du téléphone mobile, correspondant à des indications de procédure données dans un manuel du téléphone mobile, ou mieux, au cours de la session 48. Le système central 10 reçoit alors ce message, et le prend en compte au cours d'une opération 61. L'étape 61 pourra être suivie, en application du programme 17 contenu dans la mémoire 16 du système central d'une requête en vérification de code secret 62 , d'un chiffrage 63 et ou d'une vérification 64 de ce que la carte est bien détenue par son propriétaire.

L'étape 61 comporte surtout la constitution du message 5, par prélèvement des informations utiles dans la mémoire 18 (ou dans le serveur 19). L'étape 61 comporte enfin un appel du serveur 6 de la banque du commerçant. Cette étape 61 est suivie d'une étape 65 de traitement du paiement, comme dans l'état de la technique, par la banque du commerçant.

La figure 5 résume les différentes manières de mettre en œuvre l'invention. On y distingue le téléphone mobile 7, le terminal classique de paiement 1 et une carte à puce 31 utilisable pour faire fonctionner le téléphone mobile 7 et une carte à puce 2 pour payer avec le terminal 1. Selon l'état de la technique, une liaison 66 relie le terminal 1, en temps réel ou en temps différé, à un modem 67 et au serveur 6 de l'organisme financier du commerçant propriétaire du terminal 1. Selon la description précédente de

l'invention, le téléphone mobile 7 entre en relation avec les circuit 10 de l'opérateur de téléphonie mobile pour que celui-ci compose le message de paiement. Ces circuits 10 comportent une station de base 11 (propriété de l'opérateur de téléphonie mobile) et le système 12-18 de traitement évoqué ci-dessus. Dans cette première description de l'invention, le téléphone mobile 7 entre en relation avec la station de base 11 par une relation hertzienne 68.

Selon une première variante, on installe chez un commerçant une station de base privée 69. Cette station de base privée peut être mise en relation téléphonique classique, par exemple par une liaison bifilaire 70, avec le modem 67. Cette station de base privée peut par ailleurs servir d'autocommutateur pour des liaisons téléphoniques du commerçant. Selon la variante de l'invention, la station de base privée 69, entre en relation avec le téléphone mobile 7 par une liaison hertzienne privée 71. On connaît de ce point de vue, dans le domaine de la téléphonie mobile, les utilisations alternatives, publique ou privée des téléphone mobiles. Pour de telles utilisations, un porteur de téléphone mobile, arrivant par exemple à son domicile, éteint son téléphone mobile, puis le remet en service en désignant le type d'utilisation, privée ou publique. Selon le cas, le téléphone mobile cherche à alors à entrer en relation avec une station de base privée ou publique qui le capte. Puis une procédure de reconnaissance typique est lancée. Dans la pratique, il n'est même pas besoin d'éteindre le téléphone mobile, on peut lancer une procédure d'accrochage d'une base privée à partir d'une utilisation en veille dans un réseau public. Dans cette procédure, l'accrochage sur la base privée est du même type qu'un accrochage sur un réseau public, essentiellement les gammes de fréquence changent, 27 MHz ou 400 MHz pour les utilisation privées, au lieu de 900 MHz ou 1800 MHz pour les utilisations publiques.

Autrement dit, selon cette première variante, le porteur du téléphone mobile commence par quitter le réseau public, et se connecter sur un réseau privé. Ce réseau privé sur lequel il se connecte n'est pas le sien propre, mais celui du commerçant auquel appartient la station de base privée 69. Dans cette variante, le terminal 1 est aussi en relation avec la station de base 69, soit par une relation hertzienne 72, soit par une liaison filaire (non représentée). En pratique le terminal 1 et la station de base privée 69 peuvent être réalisés dans un même équipement. Dans ce cas, tous les

moyens sont réunis, chez le commerçant, pour constituer le message de paiement. En effet, selon ce qui a été décrit précédemment, le téléphone mobile connaît, et donc peut diffuser à la station de base privée 69, l'information d'identité bancaire du client débiteur. Cette diffusion sera diffusée par un sous-programme contenu dans l'opération d'accrochage du même type que la connexion spécifique vue plus haut. Le terminal de paiement 1 connaît et peut transmettre à la station de base privée 69 l'information d'identité bancaire du commerçant. Le montant de la transaction peut être indiqué par le clavier du téléphone mobile 7, ou par le clavier du terminal 1. La date peut être fournie pat le téléphone mobile 7, le terminal 1 ou même la station de base 69. Il suffit que l'un au moins de ces équipements soit muni d'une horloge temps réel. Ou encore, si la liaison 70 de la station de base 69 avec le serveur 6 est en temps réel, la date peut être fournie par le serveur 6. En remplacement de la liaison 71, complétée par une liaison 72, on peut prévoir que le téléphone mobile envoie son identité par une liaison hertzienne 73 au terminal 1. Celui ci compose alors le message de paiement et le transmet, comme avant par la liaison 66 (ou par la liaison 72) au serveur 6. Le terminal 1 et ou la station de base privée 69 peuvent dans ce cas parfaire le message de paiement.

Selon une deuxième variante de l'invention, les moyens de constitution du message de paiement pourraient être réunis autre part que chez l'opérateur de téléphonie mobile (dans les circuit 10 décrits ci-dessus) et même autre part que chez le commerçant (avec la station de base privée 69). Notamment la station de base 69 pourrait être remplacée par une station de base 11 publique. Selon cette deuxième variante cependant, le réseau public de téléphonie mobile n'intervient que pour acheminer une liaison téléphonique privée. Dans ce dernier cas, les circuits 12-18 eux (pour la partie qui concerne la construction du message 5) se trouveront dans des locaux à disposition de l'organisme financier. Par exemple, les circuits 12-18 sont situés dans un immeuble de cet organisme et relié à l'intérieur de cet immeuble par une liaison privée 75 au serveur 6. Dans ce cas l'acheteur peut, dans la rue, en remarquant par exemple une affiche publicitaire proposant un bien ou un service, acheter immédiatement ce bien ou ce service. Il compose dans ce cas avec son téléphone mobile 7 le numéro de téléphone affiché sur l'affiche publicitaire. Ce numéro de téléphone le met en

relation, via sa liaison hertzienne 74 à la station de base publique 11, et via une liaison téléphonique 76 de cette station de base 11, avec les circuits 12-18 installé dans les locaux de l'organisme financier qui gère le serveur 6. Les liaisons 74 et 76 passent, en une communication privée, sur le réseau public. Ces liaisons permettent d'établir le message de paiement puisque les circuits 12-18 comportent (par le numéro de téléphone composé dans ce cas) l'identité du commerçant par le téléphone mobile 7, l'identité du client, et, par une procédure complémentaire ou des indications préalables (0001) données par le client, le montant de la transaction envisagée.

On observera que, tant dans la version de base que dans les deux variantes, les liaisons 66, 70, 74 et 76 sont des liaisons privées. Elles sont de ce fait bien plus résistantes aux fraudes que ne pourraient l'être des liaisons de type accessibles à tous comme on en rencontre avec le réseau Internet.

De cette façon un définit avec l'invention le téléphone mobile 7 comme un terminal porteur électronique de paiement, qui possède tout ou partie des fonctions du terminal 1 classique. Selon l'invention, ces fonctions sont cependant démembrées. La constitution du message 5 de paiement est réalisée petit à petit dans le cadre de la transmission. Une permanence de l'invention est que l'identité du client est transmise par une liaison hertzienne 68, 71 ou 74 entre le téléphone mobile et le serveur 6 de la banque. Un autre moyen essentiel de l'invention est que, dans cette transmission, l'organe, le système dit central, qui reçoit cette identité au moins transmise sur une partie de son parcours par voie hertzienne, complète le message de paiement.

REVENDICATIONS

1 - Procédé de paiement électronique dans lequel

- on constitue un message (5) de paiement comportant une information d'un montant d'une transaction, une information d'identité d'un débiteur de ce montant et une information d'identité d'un créancier de ce montant,

- on envoie ce message à un serveur (6) de données d'un organisme financier,

- le serveur de cet organisme financier opère des transferts de monnaie scripturale correspondant à ce paiement,

caractérisé en ce que

- on émet (68, 71, 74) à partir d'un téléphone mobile (7), et en direction d'un système central (10) d'un opérateur (13), l'information d'identité (39) du débiteur,

- on complète (18, 19), dans ce système central, le message de paiement à partir de l'information d'identité de débiteur reçue, et d'une information d 'identité de créancier,

- on envoie le message ainsi constitué à un serveur de données d'un organisme financier.

2 - Procédé selon la revendication 1 caractérisé en ce que

- l'opérateur est un opérateur de téléphonie publique,

- au moment de l'émission (68), on émet également un code relatif à l'identité du créancier, et/ou de la transaction,

- on constitue le message de paiement à partir d'une information d'identité du créancier correspondant à ce code,

- et on envoie le message à un organisme financier correspondant à ce code.

3 - Procédé selon la revendication 1 caractérisé en ce que

- on émet (71) l'information d'identité du débiteur sur un réseau de téléphonie privée (69) du créancier,

- on compose le message de paiement dans (71-73) ce réseau, et

- on l'envoie (70) à un organisme financier du créancier.

4 - Procédé selon la revendication 1 caractérisé en ce que

- on émet (74) l'information d'identité sur un réseau de téléphonie

publique, dans le cadre d'une communication privée (75), et

- on compose et on envoie le message de paiement à un interlocuteur de cette communication privée au cours de son déroulement.

5 - Procédé selon l'une des revendications 1 à 4, caractérisé en ce que

- l'information d'identité de créancier est puisée dans une mémoire (18) du système central en utilisant le code comme adresse dans cette mémoire.

6 - Procédé selon l'une des revendications 1 à 5, caractérisé en ce que

- l'information d'identité de créancier est prélevée, en temps réel ou différé, dans une mémoire d'un serveur (19) de données du créancier en utilisant le code comme adresse, directe ou indirecte, de ce serveur de données du créancier.

7 - Procédé selon l'une des revendications 1 à 6, caractérisé en ce qu'on utilise comme identité de débiteur un numéro de compte de ce débiteur dans un organisme financier.

8 - Procédé selon la revendication 7, caractérisé en ce que

- le débiteur sélectionne dans une mémoire de son téléphone mobile une identité de débiteur à envoyer parmi plusieurs (38),

- cette identité de débiteur correspondant à un des comptes de ce débiteur dans un ou des organismes financiers.

9 - Procédé selon l'une des revendications 1 à 8, caractérisé en ce que

- dans l'information d'identité du débiteur on transmet une information d'identité proprement dite et une chaîne de caractère de cohérence, et

- on vérifie (61) dans le système central l'authenticité du message de paiement par traitement des caractères de cohérence.

10 - Procédé selon l'une des revendications 1 à 9, caractérisé en ce que

- on provoque avec le système central une session (62-64) de vérification de code secret relatif au débiteur.

11 - Procédé selon l'une des revendications 1 à 10, caractérisé en ce que

- pour envoyer le message à un serveur (6) d'un organisme financier

correspondant à ce code, le système central lit dans une de ses mémoires ou dans une mémoire d'un serveur de données du créancier des informations de connexion de cet organisme financier, et

- le système central se connecte à ce serveur de données de cet organisme financier.

12 - Procédé selon l'une des revendications 1 à 11, caractérisé en ce que

- pour émettre à partir du téléphone mobile, on enregistre préalablement dans une mémoire (35) de ce téléphone mobile les informations d'identité de débiteur.

13 - Procédé selon la revendication 12, caractérisé en ce qu'on réalise la mémoire de ce téléphone mobile sous la forme d'une mémoire amovible (31), par exemple du type carte à puce ou jeton à puce.

14 - Procédé selon l'une des revendications 1 à 13, caractérisé en ce que

- on ajoute la date au message (5) de paiement.

15 - Procédé selon l'une des revendications 1 à 14, caractérisé en ce que

- l'organisme financier correspondant au code est un organisme dans lequel le créancier a un compte.

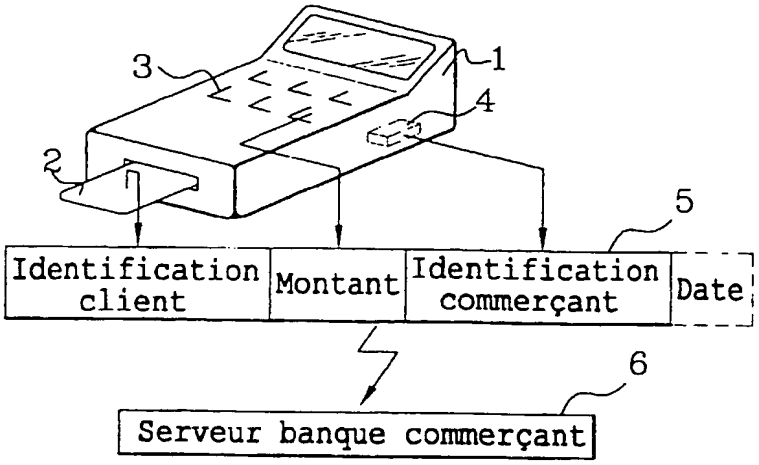

3
1
4
2
5
Identification client
Montant
Identification commerçant
Date
6
Serveur banque commerçant

FIG.1

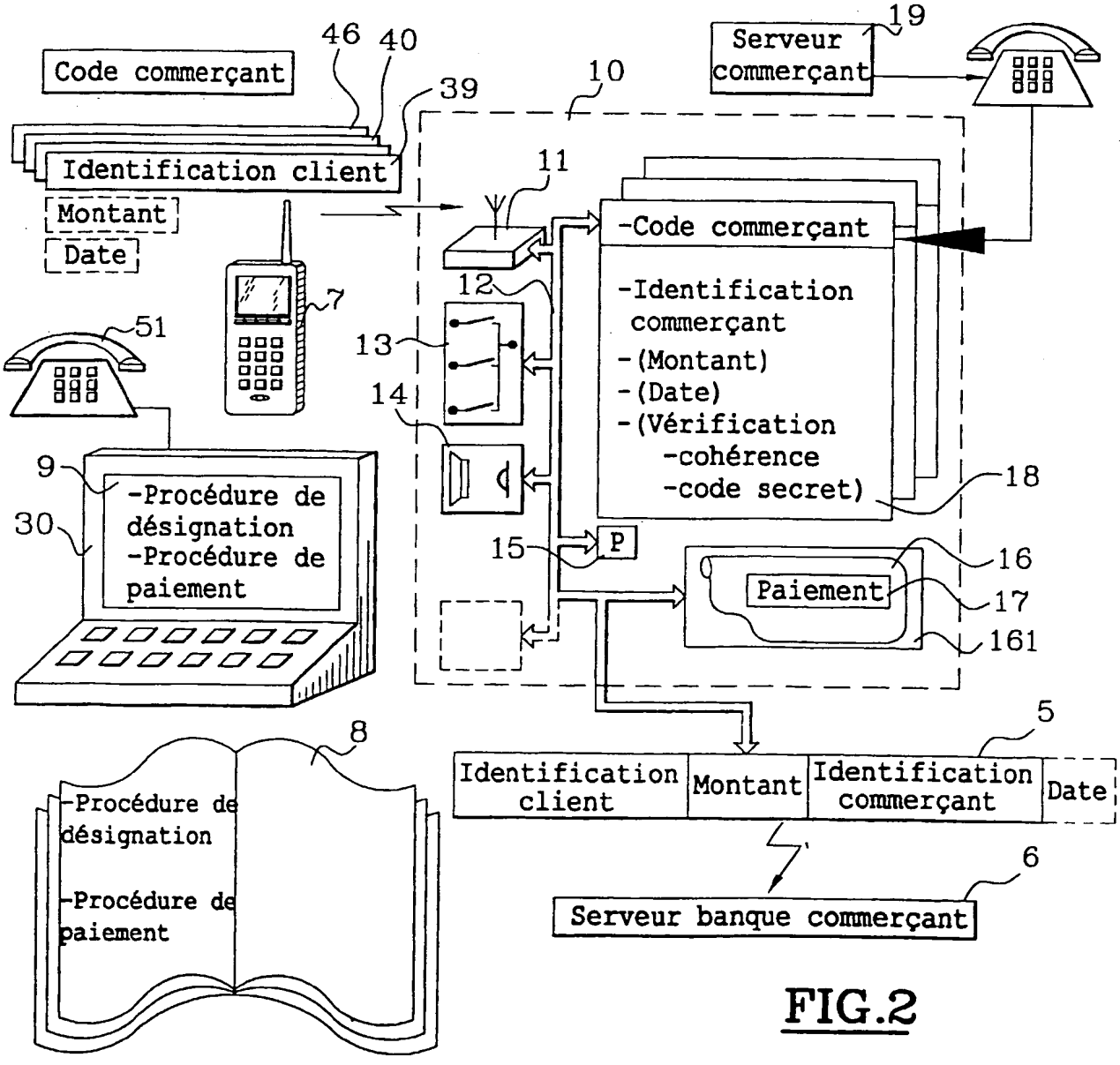
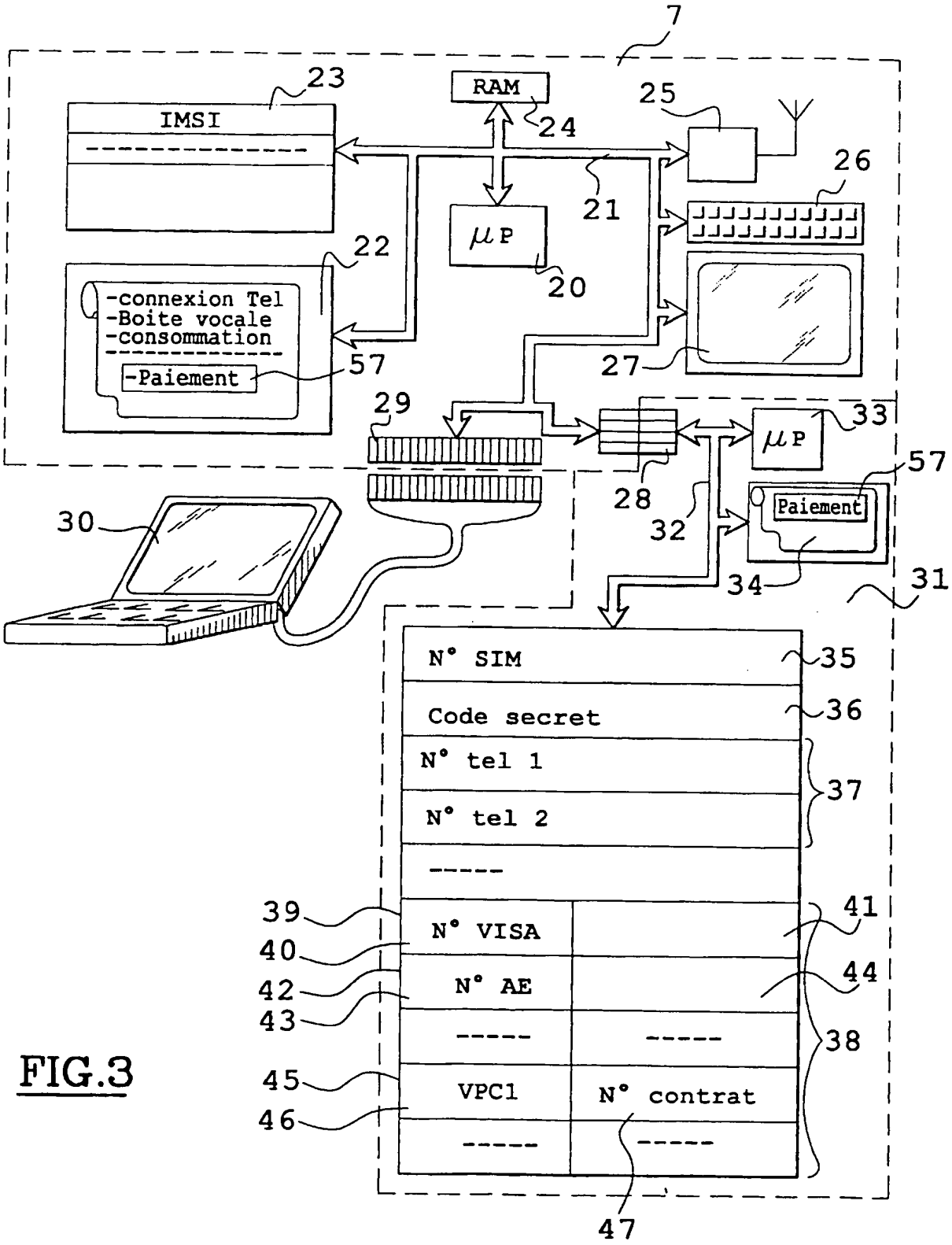

46
40
39
Code commerçant
Identification client
Montant
Date
10
Serveur commerçant
19
11
-Code commerçant
-Identification commerçant
-(Montant)
-(Date)
-(Vérification
-cohérence
-code secret)
18
12
13
14
7
51
9
30
-Procédure de désignation
-Procédure de paiement
15
P
16
Paiement
17
161
8
-Procédure de désignation
-Procédure de paiement
5
Identification client
Montant
Identification commerçant
Date
6
Serveur banque commerçant

FIG.2


7
23
IMSI
RAM
24
25
26
21
μP
20
22
-connexion Tel
-Boite vocale
-consommation
-Paiement
57
27
29
33
μP
28
32
57
Paiement
30
34
31
N° SIM
35
Code secret
36
N° tel 1
37
N° tel 2

39
N° VISA
41
40
42
N° AE
44
43

38
45
VPC1
N° contrat
46

47

FIG.3

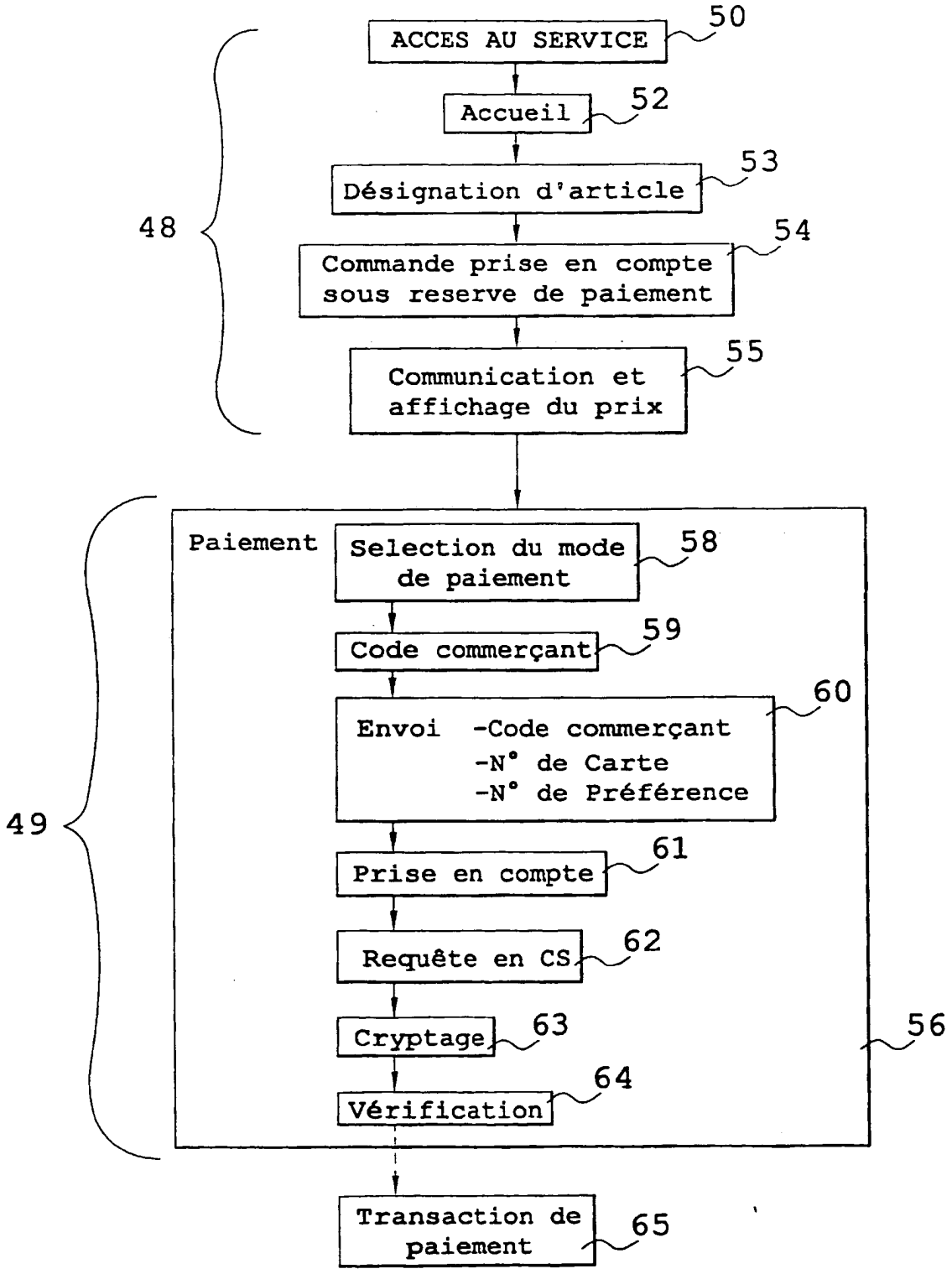

ACCES AU SERVICE
50
Accueil
52
Désignation d'article
53
48
Commande prise en compte sous reserve de paiement
54
Communication et affichage du prix
55
Paiement
Selection du mode de paiement
58
Code commerçant
59
Envoi -Code commerçant
-N° de Carte
-N° de Préférence
60
49
Prise en compte
61
Requête en CS
62
Cryptage
63
56
Vérification
64
Transaction de paiement
65

FIG.4

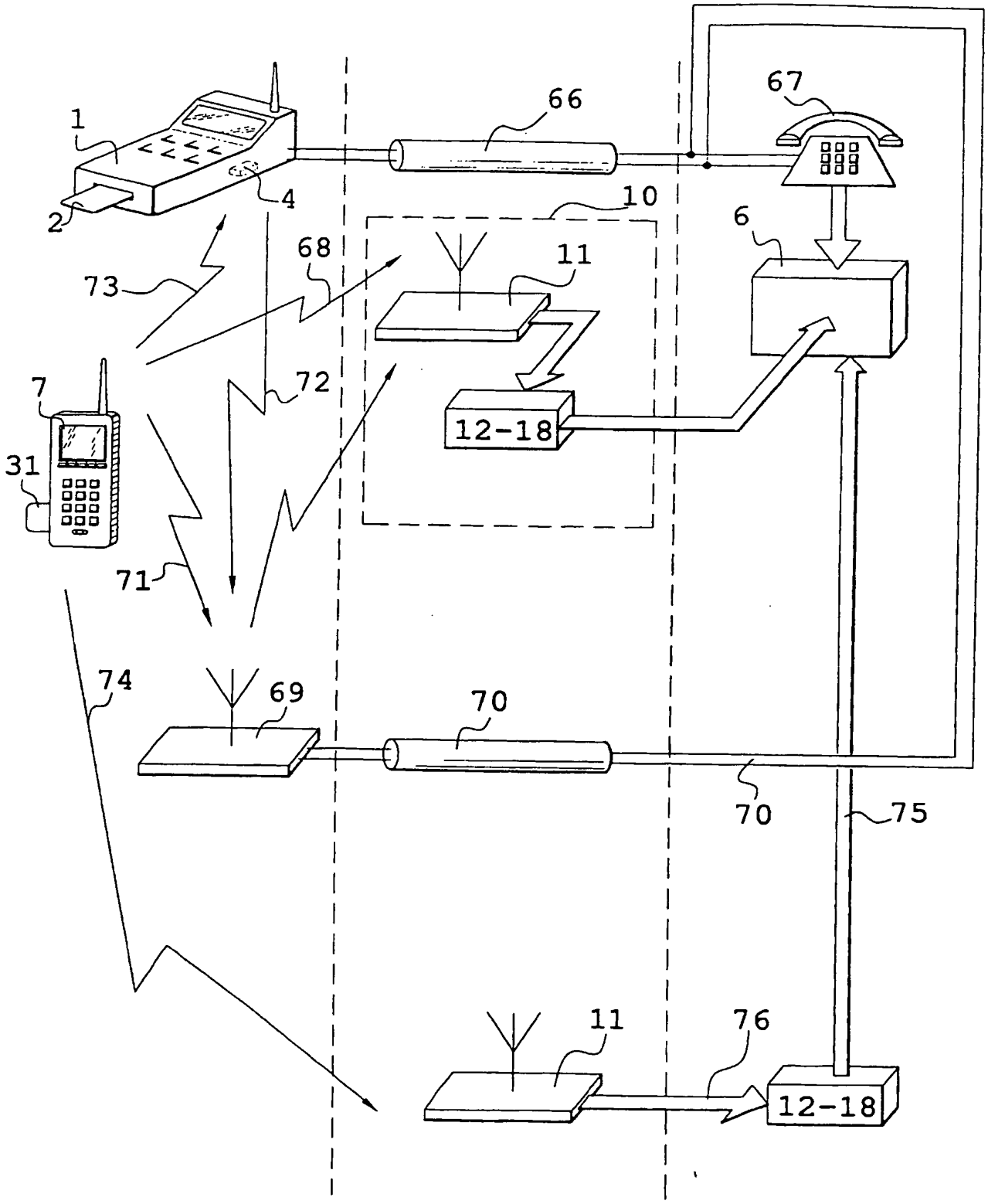


FIG.5

REPUBLIQUE FRANÇAISE

2780800

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 563494
FR 9808717

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X Y	WO 98 28900 A (RITTER RUDOLF ;PTT GENERALDIREKTION (CH)) 2 juillet 1998 * abrégé * * page 3, ligne 3 - page 7, ligne 26 * * page 9, ligne 3 - page 13, ligne 14 * * revendications; figures 1,2 *	1,2,5,9, 10 3,4,7,8, 11-15
Y	WO 96 13814 A (VAZVAN BEHRUZ) 9 mai 1996 * abrégé * * page 1, dernier alinéa - page 2, alinéa 1 * * page 3, alinéa 2 - page 4, alinéa 1 * * page 5, alinéa 3 - page 6, alinéa 1 * * revendications; figures *	3,4, 11-13,15
Y	WO 96 25828 A (NOKIA MOBILE PHONES LTD ;TERHO MIKKO (FI); HEINONEN PETRI (FI); MA) 22 août 1996	7,8
A	* abrégé * * page 3, ligne 20 - page 5, ligne 5 * * page 13, ligne 15 - page 14, ligne 3; revendications 1-4; figure 3 *	1-5
Y A	EP 0 780 802 A (AT & T CORP) 25 juin 1997 * abrégé * * colonne 6, ligne 5 - ligne 32 * * figures 1-3 *	14 1-5
A	WO 94 11849 A (VATANEN HARRI TAPANI) 26 mai 1994 * abrégé; revendications; figures *	1-15
A	EP 0 848 360 A (BRITISH TELECOMM) 17 juin 1998	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04Q
G07F

Date d'achèvement de la recherche: 9 juin 1999

Examinateur: Miltgen, E

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1